IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI WESTERN DIVISION

TUMEY L.L.P. and TOD T. TUMEY	)	
	)	
Plaintiffs,	)	
	)	
v.	)	**Case No. 4:21-00113-CV-RK**
	)	
MYCROFT AI INC., JOSHUA MONTGOMERY, and MICHAEL LEWIS	)	
	)	
Defendants.	)	

PRELIMINARY INJUNCTION

Pending before the Court is Plaintiff Tod Tumey ("Tumey") and Tumey L.L.P.'s, (collectively "Plaintiffs") Motion for Temporary Restraining Order and Preliminary Injunction, as well as Plaintiffs' Memorandum of Law in Support of that Motion. After review of that Motion, all briefing and argument of counsel, the pleadings in this case, the record, including the evidence heard during an evidentiary hearing held on March 29, 2021, and applicable law, the Motion for Preliminary Injunction is hereby **GRANTED** and Defendants are enjoined as set forth below.

I. The Court's Authority

As a threshold matter, the Court has authority to enter a preliminary injunction against all Defendants, all of whom have been served (Docs. 6, 7, and 14), and all had notice of the Motion against them (*see, e.g.*, Docs. 10 and 30). Rule 65(a)(1). In addition, Defendant Mycroft AI Inc., a corporation with its principal place of business in this district, does not contest that it is subject to personal jurisdiction here and has submitted to such jurisdiction. Mycroft has appeared in this action, opposed the Motion, and attended the hearing. Defendants Michael Lewis and Joshua Montgomery, Mycroft's CEO and First Officer, also supplied declarations in opposition to the Motion (Docs. 30-2 and 30-4), and Mr. Lewis attended the hearing via Zoom. No further

jurisdictional inquiry is necessary at this stage: Rule 65(a) authorizes the entry of a preliminary injunction upon notice to the adverse party. Rule 65(d)(2) authorizes an injunction against Mycroft to be properly applied to parties "in active concert or participation" and with actual notice – thus, the Court's issuance of preliminary injunction against Mycroft would also properly name and encompass Lewis and Montgomery upon the verified allegations and other evidence presented to the Court of their actions in concert and participation with Mycroft in this case. Fed. R. Civ. P. 65(d)(2)(C).

II. Plaintiffs Are Entitled to a Preliminary Injunction

In determining whether to issue a temporary restraining order and preliminary injunction, the Court must consider four factors: (1) the threat of irreparable harm to the movant; (2) the potential harm to the nonmoving party should an injunction issue; (3) the likelihood of success on the merits; and (4) the public interest. *See Dataphase Sys., Inc. v. C.L., Inc.*, 640 F.2d 109, 113 (8th Cir. 1981); *see also S.B. McLaughlin & Co., Ltd v. Tudor Oaks Condo Project*, 877 F.2d 707, 708 (8th Cir. 1989) (affirming a district court's application of the *Database* factors to a motion for temporary restraining order determination). "At base, the question is whether the balance of equities so favors the movant that justice requires the court to intervene to preserve the status quo until the merits are determined." *Dataphase Sys., Inc.*, 640 F.2d at 113. Further, the Eighth Circuit has made clear that "no single factor is determinative" and the court must consider the particular circumstances of each case. *Id.* Moreover, in considering these factors, the court may properly consider evidence that would ordinarily be inadmissible, such as hearsay, in support of granting temporary restraining order or a preliminary injunction. *See Ass'n of Cmty. Orgs. for Reform Now v. Scott*, No. 08-CV-4084, 2008 WL 2787931, at *3, n.5 (W.D. Mo. July 15, 2008).

Here, every one of the relevant factors supports Plaintiffs' request for entry of a preliminary injunction to protect Plaintiffs, including Plaintiff Tumey's family members, and other witnesses who participate in this case, from the retaliatory cyberattacks that are causing ongoing irreparable injury at the hands of the Defendants, and which have continued to intensify as a result of Plaintiffs' filing of the Verified Complaint.

III. There Is a Substantial Likelihood Plaintiffs Will Succeed on the Merits

Plaintiffs have shown a substantial likelihood of success on the merits of the federal Computer Fraud and Abuse Act ("CFAA") and the Stored Wire and Electronic Communications Act ("SCA") claims, as well as the common law Intrusion on Seclusion claim asserted by Plaintiff Tumey against Defendants. "[T]his circuit's ordinary preliminary injunction test . . . asks only whether a movant has demonstrated a 'fair chance of prevailing' in the ultimate litigation.'" *1-800-411-Pain Referral Serv., LLC v. Otto*, 744 F.3d 1045, 1054 (8th Cir. 2014). Plaintiffs have clearly demonstrated a "fair chance of prevailing" in the ultimate litigation against Defendants; as detailed in the 52-page Verified Complaint and the voluminous exhibits attached thereto, as well as in the Declaration of Plaintiff's cyber-defense specialist, there is compelling evidence, even at this early stage of the litigation, that the Defendants are responsible for ongoing cyberattacks and harassment against the Plaintiffs, in violation of numerous state and federal laws. *See Heartland Acad. Cmty. Church v. Waddle*, 335 F.3d 684, 690 (8th Cir. 2003) (holding that in order to obtain a preliminary injunction, a party is not required to show that it will ultimately succeed on its claims or even that it is more likely than not to succeed, but only that it has a fair chance of prevailing).

A. Plaintiffs are Likely to Prevail on the Claims under the Federal Computer Fraud and Abuse Act ("CFAA") and the Stored Wire and Electronic Communications Act ("SCA")

Under the CFAA, 18 U.S.C. § 1030, liability arises when: (1) the defendant intentionally accesses a "protected computer"; (2) without authorization or by exceeding its authorization; (3) and thereby obtains information from any protected computer. 18 U.S.C. § 1030(a)(2)(C); *see also* 18 U.S.C. § 1030(e)(2)(B) (defining a "protected computer" to include any computer "which is used in or affecting interstate or foreign commerce or communication"). Liability will additionally arise for unauthorized access to a protected computer done "knowingly" and with "intent to defraud," where, as a result, such access has "further[ed] the intended fraud and obtain[ed] anything of value." 18 U.S.C. § 1030(a)(4). Further, any "attempted" unauthorized access or conspiracies to commit such unauthorized access to a protected computer are also violations of the CFAA. 18 U.S.C. § 1030(b). The statute requires a loss in excess of $5,000 over the course of a calendar year. *Id.*; *see generally, e.g., YourNetDating, Inc. v. Mitchell*, 88 F.Supp.2d 870 (N.D. Ill. 2000) (awarding a temporary restraining order and finding a likelihood of success on the CFAA claim where it was alleged that a former programmer was "hacking" a dating service's website and diverting its clients and users to a porn site); *Reliable Prop. Servs., LLC v. Capital Growth Partners, LLC*, 1 F.Supp.3d 961, 964 (D. Minn. 2014) (granting preliminary injunctive relief and finding a likelihood of success on the merits on the alleged CFAA claim where, despite the defendant's denial that he obtained information from plaintiff's computer, "the evidence that he did so is overwhelming").

Similarly the SCA provides a civil cause of action against anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701; *id.* § 2707. An electronic communication in "electronic storage" is "(A) any temporary, intermediate storage of a wire or

electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication." 18 U.S.C. § 2510(17); *see also Cardinal Health 414, Inc. v. Adams*, 582 F.Supp.2d 967, 976 (M.D. Tenn. 2008) (noting that a case "of an individual logging onto another's e-mail account without permission and reviewing the material therein, a summary judgment finding of a SCA violation is appropriate"); *Miller v. Myers*, 766 F.Supp.2d 919, 923 (W.D. Ark. 2011) (finding an SCA violation where defendant used "a keylogger program to obtain Plaintiff's passwords . . . then used those passwords to access Plaintiff's email account without authorization").

The Verified Complaint details numerous unauthorized accesses and attempted accesses of Plaintiffs' protected computers, computer systems and computer network. (Verified Compl. ¶¶ 201-230.) Specifically, it is alleged that Defendants, on or about June 1, 2020, accessed Plaintiffs' protected computers, computer system and computer network, infiltrated information contained in one or more firm email accounts and reviewed information contained in such stored electronic communications. Defendants then used the information obtained to craft a fake email to Plaintiff Tumey, embedded with a virus, which was crafted to appear to come from Tumey's young daughter, using information pulled from emails Tumey had actually received from his daughter, to make the email appear legitimate. (*Id.* at ¶¶ 96-104.) Further, the Declaration of Plaintiffs' cyber-defense specialist details additional unauthorized accesses and attempted accesses of Plaintiffs' protected computers that are ongoing and have intensified since the filing of the Verified Complaint. (*See* Declaration of Chilton Webb).

Thus, Plaintiffs have more than satisfied its burden to demonstrate a "fair chance of prevailing on the merits" as to the CFAA and SCA claims.

B. Plaintiff Tumey is Likely to Prevail on the Claim for Intrusion on Seclusion

In addition to Plaintiffs' overall likelihood of success, including their likelihood to succeed on the alleged CFAA and SCA claims, Plaintiff Tod Tumey has also demonstrated a likelihood of success on the common law claim for Intrusion on Seclusion.

An Intrusion on Seclusion claim under Texas law requires that Plaintiff show: "(1) an intentional intrusion, physically or otherwise, upon another's solitude, seclusion, or private affairs or concerns, which (2) would be highly offensive to a reasonable person." *Buckert v. Traynor*, No. SA-19-CV-727-XR, 2019 WL 2601346, at *2 (W.D. Tex. June 24, 2019) (citing *Valenzuela v. Aquino*, 853 S.W.2d 512, 513 (Tex. 1993)).

In this case, not only is the Verified Complaint full of detailed allegations evidencing that Defendants have been behind a flood of harassing emails graphically threatening Plaintiff Tod Tumey's life (ECF No. 1 at ¶ 56-57), threatening his children (*Id.* ¶ 64), menacingly indicating an awareness of what kind of vehicle Plaintiff drove (*Id.* ¶ 61), but Defendants have also repeatedly targeted Plaintiff's immediate family members. Plaintiff Tumey's wife and daughters have repeatedly been the subject of ongoing cyberattacks since the initiation of the Patent Suits against Mycroft (*Id.* ¶¶ 8, 73, 102-104, 252-264); and now, with the filing of the Verified Complaint, it is alleged that Plaintiff's wife is once again experiencing sophisticated cyberattacks through the receipt of multiple targeted phishing emails. (*See* Chilton Webb Declaration.)

This alleged behavior is enough to constitute a likely "intrusion" on Plaintiff Tumey's "seclusion" and "private affairs" that would be "highly offensive" to a reasonable person. Such allegations are enough to establish a "fair chance of prevailing" on the merits of the Intrusion on Seclusion claim asserted against Defendants. *See e.g., Buckert*, 2019 WL 2601346, at *2 (granting a temporary restraining order where the allegations detailed ongoing harassment by defendant,

including threatening calls and social media posts, were sufficient to establish a likelihood of success on the merits for an intrusion on seclusion claim).

IV. Plaintiffs Will Suffer Irreparable Harm Without A Preliminary Injunction

Plaintiffs have also shown that they will suffer irreparable harm if injunctive relief is not granted. "To succeed in demonstrating a threat of irreparable harm, a party must show that the harm is certain and great and of such imminence that there is a clear and present need for equitable relief." *S.J.W. ex rel. Wilson v. Lee's Summit r-7 Sch. Dist.*, 696 F.3d 771, 778 (8th Cir. 2012). Irreparable harm occurs where "a party has no adequate remedy at law, typically because its injuries cannot be fully compensated through an award of damages." *Gen. Motors Corp. v. Harry Brown's, LLC*, 563 F.3d 312, 319 (8th Cir. 2009).

Plaintiffs have demonstrated they are experiencing and will continue to experience irreparable harm without immediate judicial intervention and equitable relief. Defendants are alleged to be actively targeting Plaintiffs' business and family members in retaliation for the filing of the Verified Complaint. Specifically, immediately after the first Defendant was served with the Verified Complaint on February 26, 2021, the Tumey L.L.P. servers began experiencing a significant increase in detected daily cyberattacks. (Webb Decl. at Ex. 1 ¶¶ 13, 16.) Soon thereafter, Plaintiff Tumey's wife also became a target of Defendants' sophisticated and targeted cyberattacks. (*Id.* at ¶¶ 14-15, 17.) These attacks Plaintiff's family are experiencing are ongoing. Most detrimentally, events since the filing of the Verified Complaint indicate that these recent cyberattacks may have been successful, compromising the Tumey L.L.P. firm server and email accounts, and potentially giving Defendants access to highly confidential email communications, regarding this case and others. (*Id.* at ¶¶ 18-19.)

No monetary remedy can fully compensate Plaintiff Tumey for the personal and egregious harm he has experienced and is continuing to experience through the focused and targeted cyberattacks on his family and children. Moreover, the recent events indicating that the Tumey L.L.P. firm servers are compromised, and that Defendants potentially have or had access to confidential firm email communications, is an ongoing irreparable harm that simply cannot be remedied without an immediate injunction. In order to maintain the status quo during the pendency of this litigation, and to allow the parties a full opportunity to properly litigate this matter in court, this Court cannot allow such cyber harassment to continue during the pendency of this litigation.

Moreover, this latest spike in cyberattack activity is just the most recent example of an ongoing and continuous campaign of information warfare that Plaintiffs have alleged they have experienced at the hands of the Defendants over the last twelve months. As described in the Verified Complaint, Defendants are alleged to have actively engaged in a concerted effort to access Plaintiffs' protected computers and information, which includes potential access to sensitive attorney-client privileged communications, to destroy Plaintiffs' business reputation and impede its ability to serve its clients, and to directly threaten attorney Tod Tumey and his immediate family. (ECF No. 1 at ¶¶ 52-115.) This egregious conduct has resulted in actual and threatened loss of revenue to the Tumey L.L.P. firm. (*Id.* at ¶¶ 148-151.)

Defendants' efforts to access Plaintiffs' protected computers and electronic information is ongoing and intensifying. (*See* Webb Decl., Ex. 1.) Plaintiffs have incurred and will continue to incur costs combatting and attempting to protect against these continuing cyberattacks. (ECF No. 1 at ¶¶ 148-151.) Plaintiffs have demonstrated they have experienced irreparable harm through the substantial costs it has experienced and will continue to experience attempting to defend against these ongoing cyberattacks. *See e.g., Physicians Interactive v. Lathian Sys., Inc.*, No. CA

03-1193-A, 2003 WL 23018270, at *9 (E.D. Va. Dec. 5, 2003) (granting a preliminary injunction related to alleged hacking and noting that plaintiff "has shown irreparable harm through the costs it must incur to guard against future attacks").

V. The Balance of Hardships Weighs Decisively in Plaintiffs' Favor

The balance of hardships likewise weighs in favor of Plaintiffs. In contrast to the substantial irreparable harm that Plaintiffs have demonstrated they will suffer as the result of Defendants' wrongful conduct, any harm to Defendants from a temporary restraining order and preliminary injunction would be self-inflicted and cannot be deemed irreparable as a matter of law. *See, e.g., Sierra Club v. U.S. Army Corps of Eng'rs*, 645 F.3d 978, 997 (8th Cir. 2011) (balance of harms weighed in plaintiff's favor because defendant's harm was "largely self-inflicted").

The ongoing cyberattacks against Plaintiffs are causing and will continue to cause permanent damage to Plaintiffs because once Plaintiffs' goodwill, client base, and client relations are damaged, the value of those protectable business interests may well never be restored. (ECF No. 1 at ¶ 176.) In addition, Defendants' unauthorized access and attempts to access Plaintiffs' protected computers and electronic information is alleged to have allowed Defendants to access protected attorney-client privileged information; such unauthorized access not only invades the sanctity of the attorney-client relationship, but potentially gives Defendants an unfair (and illegal) access to work-product and attorney-client privileged communications related to the active litigation matters.

In contrast, injunctive relief will merely require Defendants, and those acting in concert with Defendants, to refrain from engaging in illegal cyberattacks against Plaintiffs. While Defendants assert that they are not the perpetrators responsible for the cyberattacks experienced by Plaintiffs – if that is the case, then this preliminary injunction will have no impact on them at

all. *See, e.g., YourNetDating,* 88 F.Supp.2d at 872 (granting interim injunction restraining alleged hacking and noting that defendants "will suffer no legitimate harm of which they can complain if the interim injunction is granted because they have no honest business hacking YourNetDating's system" and further noting that defendant's concerns that "if someone else hacks the YourNetDating system in the ten days that the TRO is in force, he will be held accountable for it" were "insubstantial" compared to the risks to plaintiff).

VI. The Public Interest Favors Issuance of a Temporary Restraining Order

The public interest also favors Plaintiffs. Defendants have published statements openly warning anyone claiming intellectual property infringement by Mycroft to "not to pick fights with" them as they are skilled in "information warfare." (ECF No. 1 at ¶ 9.) Without question, the public interest is served by allowing disputes such as the patent infringement disputes between Mycroft and Voice Tech, and the dispute now between Plaintiffs and Defendants, to be resolved through appropriate judicial forums, without the attorneys attempting to advocate on behalf of their clients experiencing personal, targeted threats to their family and business. Further, this Court has an obligation to enjoin illegal behavior, including the purported hacking, harassment and witness retaliation alleged in this case. *See e.g., Physicians Interactive* 2003 WL 23018270, at *10 (granting a preliminary injunction and noting that "[t]he facts alleged by Physicians Interactive, if true, violate several federal and state criminal and civil statutes. This Court has an obligation to enjoin any alleged computer hackers from continuing to attack and steal Physicians Interactive's proprietary information.").

As such, this final factor also weighs in favor of the requested relief.

ACCORDINGLY, IT IS HEREBY ORDERED that Plaintiffs' Motion is **GRANTED.**

IT IS FURTHER ORDERED that Defendants, as well as Defendants' officers, agents, servants, employees, and attorneys, and all other persons who are in active concert or participation with any of them, shall be immediately preliminarily enjoined and restrained from:

1. Engaging in, participating in, or recklessly or intentionally inciting any cyberattacks, hacking or other harassment directed at Plaintiffs, including Plaintiffs' officers, agents, servants, employees, attorneys, witnesses and potential witnesses (including Chilton Webb and Christina Butler), and the family members of any of the foregoing (the "Protected Parties"); and
2. Using or disclosing any documents, information, or other materials of any kind obtained from Plaintiffs or any other Protected Party through any unauthorized means.

IT IS FURTHER ORDERED that, under the circumstances of this case, the terms of the injunction do not pose a material risk of any injury to Defendants, no security is necessary. Nevertheless, a bond in the amount of $ 5,000 would be more than adequate to pay the costs and damages, if any, sustained by any party found to have been wrongfully enjoined or restrained, and therefore, pursuant to Federal Rule of Civil Procedure 65, within ten days from the date of this Order, Plaintiffs shall post a bond in the amount of $ 5,000 to secure this Preliminary Injunction. In lieu of a bond, Plaintiffs may post cash or its equivalent with the Clerk of Court.

IT IS FURTHER ORDERED that this Order shall take effect immediately and, absent further Order of this Court, shall remain in effect until the conclusion of litigation in this case.

IT IS SO ORDERED.

s/ Roseann A. Ketchmark
ROSEANN A. KETCHMARK, JUDGE
UNITED STATES DISTRICT COURT

DATED: March 31, 2021